AMENDMENTS TO THE SPECIFICATION

Please cancel the heading "DESCRIPTION," in line 1 on page 1 of the specification.

Please insert the heading -- BACKGROUND OF THE INVENTION --, in line 3 on page 1 of the specification.

Please replace the heading "Technical Field," with --1. Field of the Invention-- in line 4 on page 1 of the specification.

Please replace the heading "Background Art," with --2. Description of the Related Art-- in line 13 on page 1 of the specification.

Please replace the heading "Disclosure of Invention," with --SUMMARY OF THE INVENTION-- in line 19 on page 6 of the specification.

Please amend the paragraph beginning on page 7, line 2 and ending at line 18, as follows:

In addition, to solve the problems, the present invention is a content protection system comprising a server apparatus and a terminal apparatus connected via a transmission ~~channel;~~channel, wherein the server apparatus ~~includes:~~includes a readout unit operable to read out an encrypted content and decryption information for decrypting the encrypted content from a recording medium on which the encrypted content and the decryption information are ~~recorded;~~recorded, and a sending unit operable to send the readout encrypted content and decryption information to the terminal apparatus via the transmission channel~~, and the~~. The terminal apparatus ~~includes:~~includes a receiving unit operable to receive the encrypted content and the decryption information to be sent via the transmission channel; and a decryption unit operable to decrypt the received encrypted content using the decryption information received~~, wherein the~~. The sending unit sends the decryption information via a secure transmission

channel after establishing the secure transmission channel between the server apparatus and the terminal apparatus.

Please amend the paragraph beginning on page 8, line 4 and ending at line 6, as follows:

FIG. 2 is a diagram showing a specific example of each data storing in a recording medium recorded by a playback apparatus of a device key ~~DK_1~~,

Please replace the heading "Best Mode for Carrying Out the Invention," with --DETAILED DESCRIPTION OF THE INVENTION-- in line 11 on page 9 of the specification.

Please amend the paragraph beginning on page 9, line 32 and ending on page 10 at line 25, as follows:

The recording apparatus 100 includes a device key storage unit 101 which stores a device key that each recording apparatus 100 secretly holds, a key block data storage unit 102 which obtains key revocation block data (hereafter referred to as key block data or as KB) from a key block data distribution authority 130 and stores the key block data, a media key calculation unit 103 which calculates a media key (MK) by decrypting the key block data with a device key, and a message authentication code (MAC) generation unit 104 which generates a MAC by inputting the calculated media key at the media key calculation unit 103, an encrypted content key and a MID into a one-way function~~,~~. Moreover, the apparatus 100 includes a content key encryption unit 105 which encrypts the content key inputted externally by the calculated media key (MK), a content encryption unit 106 which encrypts the content inputted externally by the content key, a secret key storage unit 107 which stores a secret key in a public key cryptosystem, a certification storage unit 108 which stores a certificate authorized with a signature by the central authority (hereafter referred to as CA) for a public key corresponding to the secret key, a CRL storage unit 109 which stores a public key certification revocation list (CRL) showing a latest list of the

revoked certifications distributed from a CRL distribution authority 140, a signature generation unit 110 which generates a signature for the media key. According to the content protection system in the present embodiment, a message authentication code (MAC) is information used for judging a validity of content in a playback apparatus 200.

Please amend the paragraph beginning on page 11, line 15 and ending on page 12 at line 19, as follows:

The playback apparatus 200 includes: a device key storage unit 201 which stores a device key secretly held in each apparatus; a media key calculation unit 202 in which a media key (MK) is calculated by decrypting the key block data read out from the recording medium 120 with the device key; and, a message authentication code generation unit 203 in which a message authentication code is generated according to the one-way function by using ~~following three information~~: the media key (MK) obtained at the media key calculation unit 202, a media ID obtained in the media ID recording area 121 in the recording medium 120, and the encrypted content key recorded in the encrypted content key recording area of the recording medium 120~~;~~. Moreover, the apparatus 200 includes: a content key decryption unit 204 in which the encrypted content key read out from the recording medium 120 with the calculated media key is decrypted; a content decryption unit 205 in which the encrypted content read out from the recording medium 120 with the decrypted content key is decrypted; a CA public key storage unit 206 in which a public key of the CA is stored; a certification verification unit 207 which verifies the validity of the certificate read out from the recording medium 120 using the public key of the CA, that is, verifying the signature given on the certificate~~;~~. Furthermore, the apparatus 200 includes a CRL storage unit 208 in which the latest CRL to be obtained from the CRL distribution authority 140 is stored; a CRL verification unit 209 which verifies the validity of the CRL read out from the recording medium 120 using the public key of the CA, that is, verifying the signature given on the CRL; a CRL comparison/updating unit 210 which compares old and new of the CRL to be stored in the CRL storing unit 208 with the CRL whose validity is examined after reading out from the recording medium 120 and stores the newest CRL into the CRL storing unit 208; a certification judgement unit 211 which judges whether or not the

certificate read out from the recording medium 120 is registered on the newest CRL stored in the CRL storing unit 208; a signature verification unit 212 which verifies a signature read out from the recording medium 120 using the certificate read out from the recording medium 120; and a switch 213 which is controlled based on a result of the ~~judgement~~ judgment and a number of verifications.

Please amend the paragraph beginning on page 19, line 6 and ending at line 9, as follows:

The above discussion explained the CPS-2 recording method for the content protection system according to the present embodiment. Next, the recording apparatus 100 and the content protection system according to the present invention are explained.

Please amend the paragraph beginning on page 19, line 17 and ending at line 24, as follows:

Further, as the plurality of the content protection recording methods according to the present embodiment, ~~three methods of~~ the conventional CPRM recording method, the above-mentioned CPS-2 recording method according to the present embodiment, and a Non-CP recording method are used for an explanation. However, the recording apparatus 100 ~~does not limit~~is not limited to these three methods, but it is adoptable to the plurality of recording methods using other content protection systems.

Please amend the paragraph beginning on page 20, line 1 and ending at line 14, as follows:

The receiving unit 301 receives an encrypted content via a net distribution, a digital broadcasting, a DVD, and the like. In addition, the control unit 302 includes: a recording medium identification unit 302a which identifies whether the recording medium 120, via the R/W unit 305, is able to correspond to a CPRM recording method, a CPS-2 recording method, or a Non-CP recording method; a source identification unit 302b which identifies a type of the source based on whether the received content is for the content protection or not; a recording method selection unit 302c which

selects the content protection method by the recording apparatus 100 on the recording medium 120 out of the CPRM recording method, the CPS-2 recording method, or the Non-CP recording method; and a recording method conversion unit 302d which ~~coverts~~ converts these three recording methods.

Please amend the paragraph beginning on page 20, line 15 and ending at line 20, as follows:

The input unit 303, such as a keyboard, inputs a selection of a content protection recording method by a user of the recording apparatus 100 on the recording medium 120 of the content. Further, the memory unit 304 is a hard disk memorizing the encrypted content 300 and the like which the receiving unit 301 received.

Please amend the paragraph beginning on page 21, line 20 and ending on page 22 at line 1, as follows:

Consequently, the recording medium 41 is allowed to correspond to all three content protection recording methods: the CPRM recording method which requires both MID and KB, the CPS-2 recording method which requires only MID, and the Non-CP recording method which does not provide a content protection~~; the~~. The recording medium 42 is allowed to correspond to two of the content protection recording ~~methods:~~methods, the CPS-2 recording method and the Non-CP recording method~~; and the~~. The recording medium 43 is allowed to correspond only to the Non-CP recording method. Accordingly, the recording method selection unit 302c in the recording apparatus 100 is allowed to select a recording method of content according to the types of the recording medium 41 and the like. In addition, it is shown as NG when content cannot be recorded on a recording medium by the recording apparatus 100.

Please amend the paragraph beginning on page 22, line 7 and ending at line 17, as follows:

In FIG. 5, the recording apparatus 100 is shown that its type of a recording medium is a recording medium 41 that a media ID (MID) and a key block (KB) Data are written in its non-

rewritable area, and ~~in the case where~~when the type of its receiving source is a net distribution, the recording apparatus 100 selects its content recording method on the recording medium 41 out of the following three recording methods: the CPRM recording method, the CPS-2 recording method, and the Non-CP recording method. Thus, the recording apparatus 100 corresponds to a multi-disk on which content can be recorded according to a plurality of the recording methods.